社会インフラを担うセキュリティ人財育成の課題と日立の取り組み

サイバー攻撃とセキュリティ脅威の増大に伴い，それに対応できるセキュリティ人財が不足し，国内外でセキュリティ人財の育成が注目されている。IoT時代の社会インフラを提供する事業者として，日立においてもセキュアな製品サービスの提供や業務システムの運用ができる人財の育成が急務となっている。
本稿ではセキュリティ人財育成の課題を俯瞰し，セキュリティ人財に対する産学官での連携や日立グループでの取り組みを示し，顧客と連携するセキュリティ人財育成について提案する。

對馬 孝高 | Tsushima Yoshitaka
藤山 達也 | Fujiyama Tatsuya
夏目 学 | Natsume Manabu
坂倉 基司 | Sakakura Motoshi
仲野 亮 | Nakano Ryo

1. はじめに

1.1 サイバーセキュリティの動向

かつてのサイバー攻撃は興味本位の愉快犯によるものが主であったが，現在は金銭目的，あるいは諜(ちょう)報・軍事といった明確な目的をもって行われている。同時に攻撃手法が高度化しており，大規模，無差別な攻撃とともに，特定の対象を狙った執拗（よう）な攻撃も見られる。

近年のサイバー攻撃には，ランサムウェアによるコンピュータ上のデータを破壊する攻撃がある。2017年5月のWannaCryによる被害は国内でも見られ，6月にはNotPetyaが東欧を中心に猛威を振るった。これらの被害はIT系に限らず，製造業や電力事業などの制御システム（OT：Operational Technology）分野においても生じており，業務に多大な影響を与えた。

IoT（Internet of Things）デバイスが普及しつつあるが，それらのセキュリティ対策は不十分な場合があり，マルウェアMiraiや亜種による被害では多数のIoTデバイスがボット（攻撃の踏み台）として大規模なDDoS（Distributed Denial of Service）攻撃に悪用された。

また，脆（ぜい）弱性が悪用された攻撃事例も非常に多く，Webサーバで利用されるWordPressやApache Struts2の脆弱性に対する攻撃事例が多発した。さらに，ソフトウェアに限らず，投機的実行を行うCPU(Central Processing Unit）での脆弱性であるMeltdownやSpectreも公開され広く報道された。脆弱性は経時とともに発見されるものであり，その対策も継続的に行う必要がある。

現在は幅広い業種で，業務遂行のためにITが不可欠である。また，IoTなど新領域での活用も進んでいるが，それらは必ずしも適切なセキュリティ設計・管理がなさ

れているとは限らず，サイバー攻撃のリスクは依然として増大し続けている。

1.2
セキュリティ人財の不足

サイバー攻撃のリスクは増大する一方だが，サイバーセキュリティ対策を担う人財は不足していると言われている。

経済産業省が2016年6月に公開した調査[1]では，2014年時点で8.2万人不足していたセキュリティ人財が2016年時点で13.2万人の不足に達し，2020年時点では19.3万人まで拡大すると報告している。

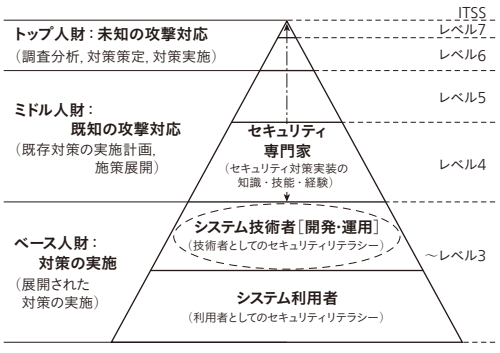
また，IPA（Information-technology Promotion Agency, Japan：独立行政法人情報処理推進機構）がとりまとめて選考している「情報セキュリティ10大脅威 2018」では，組織の10大脅威の第5位として「セキュリティ人材の不足」が挙げられており，セキュリティ人財不足が組織に対する脅威として取り上げられる状況となっている[2]。

セキュリティ人財の不足傾向は国内に限らず海外でも同様である。昨今のサイバーセキュリティ情勢に対応するためにはセキュリティ人財の育成が急務である。

1.3
求められるセキュリティ人財像

セキュリティの確保は一部のセキュリティ専門家だけでは実現不可能であり，組織の構成員が担当業務に応じてそれぞれセキュリティ面での役割を果たす必要がある（**図1**参照）。そのためには，スキルセット（知識）はもちろんだが，マインドセット（意欲）も同様に重要である。

図1｜セキュリティ人財像
おのおのの役割に応じたセキュリティ知識の習得が必要である。



注：略語説明
ITSS（Information Technology Skill Standard：ITスキル標準）

一般のシステム利用者は，安全にシステムを利用するための知識，意欲を持たなければならない。

システム技術者は，指示されたセキュリティ対策を的確に遂行できる必要がある。加えて，各システム固有のリスクに応じて，自主的なセキュリティ対策を推進できることが望ましい。

セキュリティ専門家は，セキュリティ対策の立案・展開や対策の必要性を訴求する能力も必要である。

1.4
人財育成の課題と解決の方向性

役割に応じて必要とされるセキュリティの能力は異なるため，人財育成を行う際には階層，役割ごとに適した研修，研鑽（さん）のやり方を用意しなければならない。

セキュアなシステム構築にはセキュリティとその他のITスキルなどの多様な専門性を持つ人財が必要となる。また，セキュリティは範囲が広く全領域に精通することは困難である。そのため，セキュリティに関する全般的な知識を持ったうえで得意分野を深化させることとなる。

セキュリティ人財の育成に際しては上述の点を考慮する必要がある。しかしながら，セキュリティは内容が多岐に渡るうえその変化も激しい。一企業での対応は限界があるため，共通的な取り組みについては各界が連携して社会として対処していくことが重要である。

2. 産学官でのセキュリティ人財育成

安定したセキュリティ人財確保にはさまざまな分野での人財育成施策が必要であり，社会全体で取り組む必要がある。本章では産業界，学術界，行政が連携した人財育成への取り組みを紹介する。

2.1
中核人材の育成
～産業サイバーセキュリティセンター～

重要インフラ・産業基盤においても安全が脅かされる事案が発生している。それらの領域でのサイバーセキュリティ対策を強化すべく，IPA内に「産業サイバーセキュリティセンター」を日立製作所 取締役会長の中西宏明をセンター長として開設した。同センターでは，「人材育成事業」，「実際の制御システムの安全性・信頼性検証事業」，「攻撃情報の調査・分析事業」を中核の事業としている。ここではその中の一つである人材育成事業につ

いて紹介する。

社会インフラ・産業基盤でのセキュリティ対策には，情報（IT）系システム，制御（OT）系システム双方のスキルが要求される。また，適切な対策には自社システムのリスク認識とセキュリティ対策判断が可能な人財が必要である。それらの人財育成のために「中核人材育成プログラム」と「短期プログラム」の2種のプログラムを用意している。

中核人材育成プログラムは，将来的に経営層と現場担当者をつなぐ「橋渡し人材」の育成を目的とした1年間の長期プログラムであり，テクノロジー，マネジメント，ビジネス分野のスキルを総合的に学習する。テクノロジー（OT・IT）分野では，座学，机上演習，ハンズオンでの基礎的演習に加えて模擬システムを利用した実践的演習も含まれ，セキュリティ理論，攻撃・侵入手法，インシデント対応を学ぶ。また，マネジメント，ビジネス分野では，橋渡し人材として現場から経営層までの幅広い視点を備えられるようにする。加えて，海外機関との連携トレーニングにより，スキルだけではなく国境・業種を越えたトップレベルの人脈形成を実現するカリキュラムとしている。なお，本プログラムには日立からも5人が参加している。

短期プログラムは数日間のトレーニングで，CISO（Chief Information Security Officer：最高情報セキュリティ責任者）などのセキュリティ担当経営層を対象とした業界共通の内容と，CISO補佐要員を対象とする業界別の内容の2種を用意しており，自社の課題把握や国内外動向の把握，他社やセキュリティ有識者との人脈形成をめざしている。

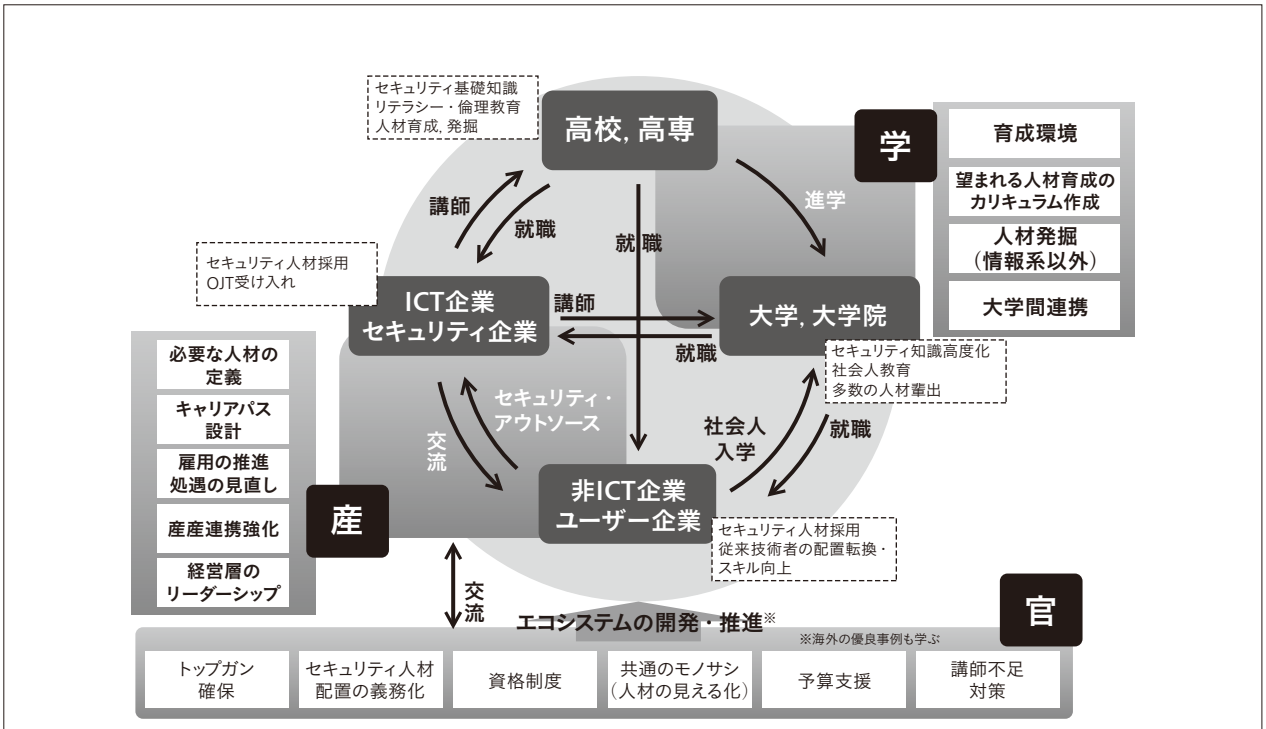
2.2
人財育成の枠組み作り
～産業横断サイバーセキュリティ人材育成検討会～

サイバーセキュリティの確保は，重要インフラ関係企業だけでなく，すべての企業にとって信用の維持や事業の継続に関わる重要な課題である。

日本経済団体連合会（以下，「経団連」と記す。）では「サイバーセキュリティに関する懇談会」を開催し，「サイバーセキュリティ対策の強化に向けた提言」を公開した。この提言の一つに，産業界に対してサイバーセキュリティを経営課題として捉え，人材育成などの取り組みを推進することが盛り込まれた。これを受けて日本電信電話株式会社，日本電気株式会社，および日立製作所の3社が発起人・事務局となり「産業横断サイバーセキュ

図2｜人材育成・維持のためのエコシステム

おのおのの役割に応じたセキュリティ人材育成が必要である。産業横断サイバーセキュリティ人材育成検討会では，将来的にはサイバーセキュリティ人材育成・維持のためのエコシステム（人材を育成・雇用・活用し続ける循環）の実現をめざす。



注：略語説明
OJT（On the Job Training），ICT（Information and Communication Technology）

リティ人材育成検討会」を発足した。

この検討会では重要インフラ分野を中心としたユーザー企業が結集し，産業界におけるセキュリティ人材育成（育成と雇用）の在り方などについて検討を行ってきた。

検討の結果，産業界が必要とする人材像の定義・見える化の枠組みとして，産学官連携を前提とした「人材育成・維持のためのエコシステム」を策定し（**図2**参照），活動報告書として公開した。この検討結果は経団連からも賛同が得られており，経団連が発行した提言「Society 5.0実現に向けたサイバーセキュリティの強化を求める」に採用された[3)]。

本検討会は継続してこのエコシステムの実現に向けて議論を推進しつつ，活動結果の産業界への展開を図る。企業の実状に合った人材育成の具体的な施策として実装され，サイバーセキュリティの水準向上に貢献することを期待する。

2.3
学生向けセキュリティ教育　～高専人財の育成～

近年，高等専門学校（以下，「高専」と記す。）の輩出人財が，その確かな専門知識と技術力から，注目を集めている。全国51高専を運営する独立行政法人国立高等専門学校機構（以下，「国立高専機構」と記す。）では，セキュリティ人財不足の対策に「15歳からの情報セキュリティ人材育成」で貢献するため，情報セキュリティ人材育成事業（通称K-SEC）を展開している。そこに日立も連携し，高専輩出人財の到達目標の明確化と，教材開発に協力した。

具体的な取り組みの一つが，直接高専を訪問して行う出前授業である。国立高専機構との議論のうえ選定した7つのセキュリティ講座に対し，日立が持つセキュリティ教育の知見を基に，学生向け教材を新規に開発し，K-SECの2017年度拠点校の一つである一関高専にて，実際に授業を行った。**表1**に出前授業の講座名一覧を示す。学生からは「難しかったが，ためになった」と好評を得た。

表1｜**出前授業講座名一覧**
一関高専にて開催した授業の一覧を示す。

No.	講座名
1	情報セキュリティリスクの基礎
2	暗号理論と応用
3	ハードウェアセキュリティ
4	ネットワークセキュリティ
5	ソフトウェアセキュリティ
6	情報セキュリティと法制度
7	情報セキュリティマネジメント

もう一つの取り組みが，高専生を対象としたインターンシップである。日立のセキュリティ人財育成業務の一部として，SE（Systems Engineer）向けのWebアプリケーションなどの脆弱性を突いた攻撃への対策教材作成をテーマに実施した。参加学生からは，「サイバー攻撃の怖さを実感し，セキュリティの重要性が十分に理解できた」という感想があった。また，セキュリティの現場に触れたことで，目標の人財像が明確になり，インターンシップ参加前よりも前向きに学習できているという報告を受けている。

これらの取り組みを通してセキュリティ人財に至るための土壌を醸成し，若年層から継続的に，基礎から実践に至るまでセキュリティを学べるようにすることで，セキュリティ人財不足の解消につながることを期待する。

3. 日立のセキュリティ人財育成

産業界でのセキュリティ人財育成の事例として，日立におけるセキュリティ人財の見える化（評価）と育成制度について紹介する。

3.1
人財の評価と発掘　～ITSSレベル診断とCIP制度～

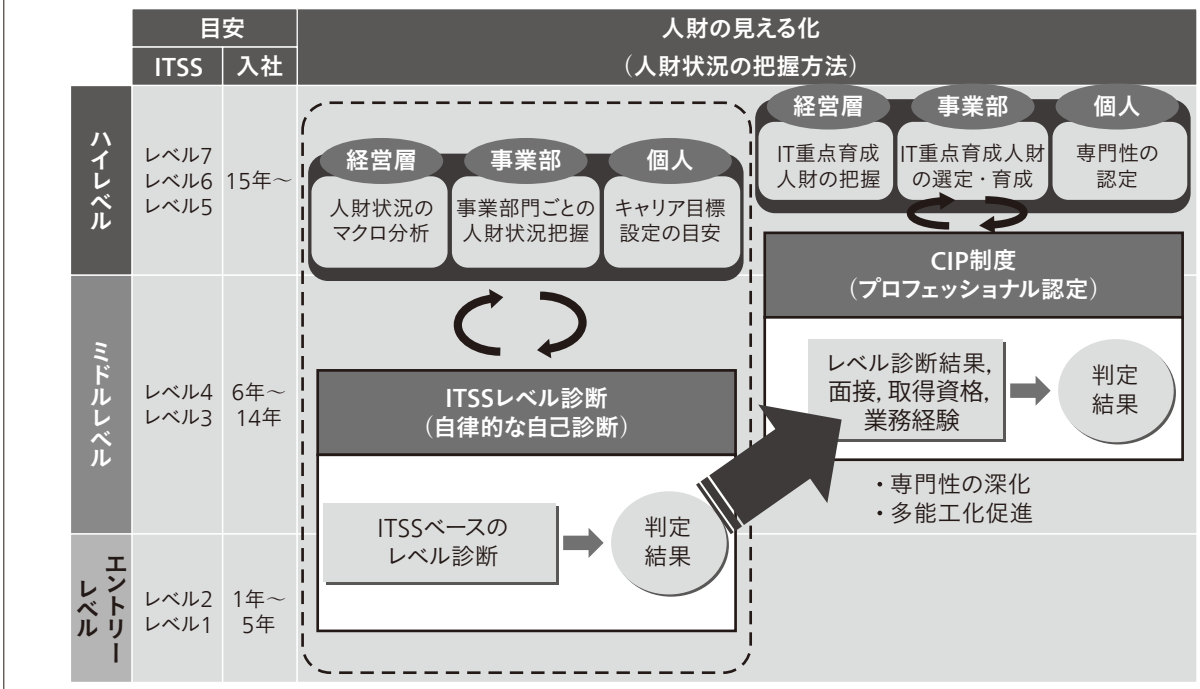
日立では，ITSS（Information Technology Skill Standard：ITスキル標準）レベル診断と日立ITプロフェッショナル認定（CIP：Hitachi Certified IT Professional）制度の2つの仕組みを併用して人財状況を把握している（**図3**参照）。

ITSSとは，経済産業省が定めたIT関連サービスの提供に必要な実務能力を明確化・体系化した指標であり，専門分野ごとに達成度指標，スキル，習熟度を7段階のレベルで定義した，IT市場共通の尺度に基づくスキル評価指標である[4)]。日立でのITSSレベル診断は，個々のスキルに関する設問に本人が回答し，その内容を上長が確認のうえ承認してITSSレベルが確定する。ITSSではITスペシャリスト（セキュリティ）などの複数職種が定義されており，評価結果はITエンジニアのスキル把握，業務アサインメントおよび業務遂行に必要なスキル習得計画の策定に活用している。

一方，CIP制度は高度ITプロフェッショナル人財（ITSSレベル4相当以上）を認定する，日立の社内認定

図3｜ITSSレベル診断とCIP制度の関係

ITSSレベル診断は自己診断主体であるのに対し，CIP制度は資格などのスキル要素と業務経験などのキャリア要素に基づいて第三者評価にて判定する。



注：略語説明
CIP（Hitachi Certified IT Professional）

制度である。社内制度ではあるが，情報処理学会が推進する「認定情報技術者制度」と同等の水準との企業認定を受けており[5]，公的な資格に準ずる。

認定に際しては研修受講や公的資格といったスキル要素に限らず，業務経験やプロフェッショナルとしての社会貢献といったキャリア要素についても評価を行い，高度な技術者には後進の育成や情報発信などの周囲も成長させる取り組みを求めている。なお，本認定の有効期限は3年間であり，認定更新の要件として継続的な研鑽や社内外への貢献，業務経験を要求している。

ITSSと同様にCIP制度でも複数職種を定義しており，セキュリティに関連する職種として日立認定情報セキュリティスペシャリストを定義している。

このように日立では，エントリーレベルからミドルレベルの評価にITSSを，それ以上のレベルの人財評価にCIP制度を利用し，社内でのセキュリティを含むIT人財の見える化，発掘，育成推進と活用を図っている。

3.2
社内セキュリティ研修の企画と運営

日立では，セキュリティ要素技術を取り扱う研修と開発・運用プロセスに対応した研修を整備している（**図4**参照）。セキュリティに関する動向の変化は激しく，特に技術研修では変化に追従しないとすぐに研修内容が陳腐化する。このため，日立ではセキュリティ技術研修内容の改訂や新規研修を企画運営する委員会組織を設立し，定期的な講座体系の見直しを実施している。

委員会はSE部門，開発部門，制御部門，セキュリティ技術部門，品質保証部門などの関連する部門から有識者を集めて構成しており，セキュリティ動向に沿った，現場が必要とする内容を研修に取り込んでいる。

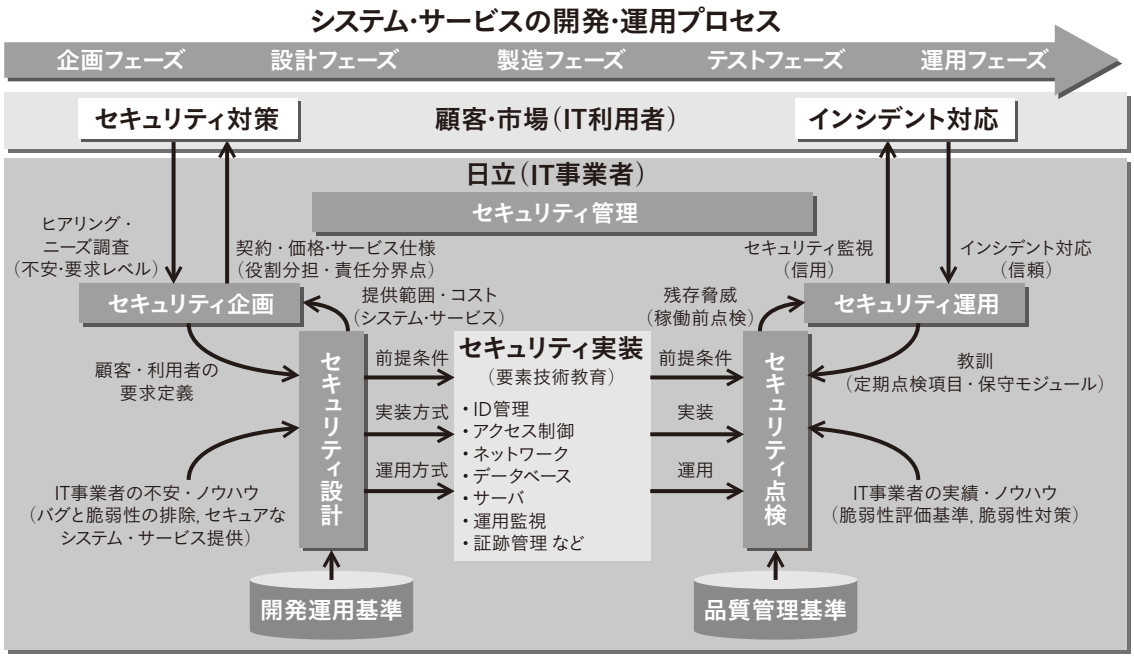
3.3
講師育成と継続研鑽　～実習とコミュニティ～

万が一のセキュリティインシデント発生時に適切な対応を実現するには，各部門での訓練が必要となるが，研修講座によるセキュリティ技術の指導は講座数，受講者数が限られる。また，部署により業務の特徴が異なるため，最適な訓練にはそれらを加味することが望ましい。

このため，日立ではセキュリティを教えることができる人財の育成を目標とした実習講座を用意している。本講座では適切なセキュリティ事故事例の選定や，その原因分析とシナリオ化を行い，セキュリティインシデント対応訓練を自身で企画し，教材作成，教育担当ができるスキルを身につけた講師を育成する。これにより各部署でのインシデント対応啓発推進を図る。

図4｜開発・運用プロセスとセキュリティ技術研修

開発・運用プロセスに対応したセキュリティ技術研修を整備している。



また，ある程度のセキュリティスキルを身につけた人財は，研修の受講だけではそれ以上の成長は難しい。このため，「プロがプロを育てる」をコンセプトとして，セキュリティ関連情報やノウハウのハブとなるコミュニティサイトを用意した。このコミュニティサイトは前述の日立認定情報セキュリティスペシャリストを中心とした社内有識者が利用可能であり，有識者どうしの意見交換，コミュニケーションを通じた相互の成長を期待している。

4. 顧客と連携したセキュリティ人財育成

日立は，社内セキュリティ人財育成を推進するとともに，各界と連携した取り組みにも参画している。これらの知見を生かし，顧客先での人財育成を支援するサービスを提供することで，社会のセキュリティ向上に貢献する。

4.1
重要インフラ事業者向け研修　～OT人財の育成～

重要インフラや産業基盤といった制御システム（OT）分野においても，セキュリティリスクの高まりを受け，サイバーセキュリティ対策の強化が求められている。対策の観点として，攻撃監視・検出，防止・対処などの技術的な対策だけではなく，攻撃に対処する人財の育成や組織強化も重要である。

OT分野でのセキュリティ対策を担う人財はセキュリティの知識だけではなく，守る対象となる制御システム（OT）および業務システム（IT）双方に精通し，固有のリスクを把握したうえで対応できる必要がある。

日立は，社会インフラシステムの開発･製造を長年担っており，その技術・ノウハウを活用したOT分野でのサイバー防衛訓練のための施設，NxSeTA（Nx Security Training Arena）を2017年8月に設置した。

本施設では顧客の実環境を模擬したOT，ITシステム環境を構築し，人財や組織の強化に着目した実践的な訓練を行うことができるサイバー防衛訓練サービスを提供している（**図5**参照）。

訓練カリキュラムは以下から構成される。

(1) 講義

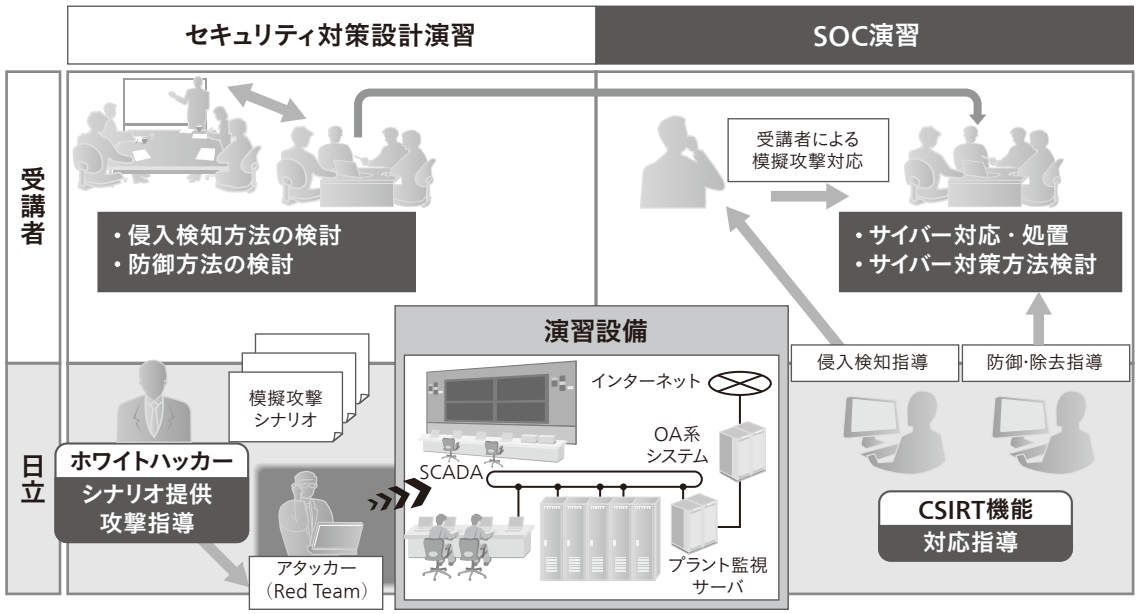
訓練で使用するシステムについての学習と，ITおよびOTシステムでのセキュリティの基礎知識，セキュリティインシデントの最新事例について学習する。

(2) ワークショップ

システム構成図を見ながら想定されるリスクを抽出する。また，それに対する検知・防御方法を検討し，リス

図5｜NxSeTAの活用シーン

受講者一人ひとりに役割を設定し，全員が組織的な対応を体験するサイバー攻撃の模擬演習を実施する。



注：略語説明
SOC（Security Operation Center），CSIRT（Computer Security Incident Response/Readiness Team），SCADA（Supervisory Control And Data Acquisition），OA（Office Automation）

ク分析手法を学ぶ。

(3) ハンズオン

演習用ネットワークで，実際の攻撃手法と攻撃に対する防御方法を実践的に学ぶ。

(4) シナリオ訓練

受講者はITまたはOTシステムの担当者の役割を担い，アタッカー役からの攻撃に対処する。もしくは経営層やマネージャの役割を担い，システム担当者からの報告を基にして事業継続可否を判断する。

これらのカリキュラムを通じてサイバー攻撃に対してどのように対応・判断していくかを実践的に体験・訓練し，組織としての対応能力向上をめざす。なお，カリキュラムは顧客に応じてカスタマイズしたうえで提供している。

日立は，OT分野においても技術面だけではなく，人財面も含めたセキュリティ確保・向上に顧客とともに取り組んでいく。

4.2
IT利用者向け研修　～IT人財の育成～

日立社内のセキュリティ人財育成の取り組みのうち，社外に対する提供を検討しているものを本節で紹介する。

日立では，サイバー攻撃の概要とインシデント発生時の対応心得の把握を目的とした研修を幅広い要員に対して実施している。本研修は技術面の知識習得も含むが，マインドセットに重点を置いている。共通的なセキュリティ研修は統制面（ルールに基づいた禁止事項の列挙）に偏りがちだが，本研修では行動がもたらす結果を理解したうえで適切な対応を身につけることをめざしている。

(1) サイバー攻撃対応基礎知識修得

基礎知識編と体験学習編で構成されるeラーニングで，前者では基本的なサイバー攻撃の手口と対策，インシデント発生時の専門家との連携方法の再確認などの基礎知識習得を図る。後者では，サイバー攻撃を具体的にイメージできるよう，動画での疑似体験を行う。標的型攻撃やランサムウェア感染などの4パターンのインシデント事例を取り扱っており，どの行動が事故につながったか，受講者に実感を持たせる。また，その際に取るべき行動を検討し，適切な対処ができることをめざす。

(2) サイバー攻撃対応コミュニケーション訓練

トレンドマイクロ株式会社のカードゲームを活用した，想定環境での役割分担を決めて行うロールプレイ形式のグループ演習である。受講者は，断片的なインシデントの情報から発生事象の想定とその影響把握，対策の

検討と専門家との連携を訓練する。サイバー攻撃への感度を上げて参加者間でリスクを共有することと，問題発生時には躊躇（ちゅうちょ）なく専門家や関連部門に報告・連絡・相談をして，適切な対処を取れるようになる事をめざす。

コミュニケーション訓練研修を行うにあたって，想定環境が一般的なものでも効果はあるが，受講者の身近な環境を想定した方がより効果的である。また，顧客先で研修を広く展開するに当たっては，組織内の事情を熟知している顧客が講師を務め，キーパーソンとなることが望ましい。このため，講師育成を目的とした実習講座の社外向け提供も併せて検討している。

社会のセキュリティ向上・底上げのため，共通的なセキュリティの啓発については積極的に社外との連携を図り，顧客との協創につなげていく。

5. おわりに

本稿では，セキュリティ人財育成に関する産学官で連携した取り組みや日立社内での取り組みを紹介した。

日立は，今後も提供する製品・サービスでのセキュリティ確保はもちろんのこと，社会全体のセキュリティ向上・底上げに取り組み，進展するデジタル社会が安全・安心なものとなるよう継続して取り組んでいく。

参考文献など

1）経済産業省：IT人材の最新動向と将来推計に関する調査結果（2016.6），
http://www.meti.go.jp/policy/it_policy/jinzai/27FY_report.html

2）IPA（独立行政法人情報処理推進機構）：情報セキュリティ10大脅威 2018，
https://www.ipa.go.jp/security/vuln/10threats2018.html

3）産業横断サイバーセキュリティ人材育成検討会，
http://cyber-risk.or.jp/

4）IPA（独立行政法人情報処理推進機構）：ITスキル標準とは?，
https://www.ipa.go.jp/jinzai/itss/itss1.html

5）一般社団法人情報処理学会：認定情報技術者制度，
https://www.ipsj.or.jp/citp.html

執筆者紹介

對馬 孝高
日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
サイバーセキュリティ技術本部 セキュリティ人財統括センタ 所属
現在，サイバーセキュリティ人財育成・評価業務に従事
CISA，CISM，CISSP

藤山 達也
日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
サイバーセキュリティ技術本部 セキュリティ人財統括センタ 所属
現在，サイバーセキュリティ人財育成・評価業務に従事
CISSP

夏目 学
日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
マネジメント本部 セキュリティ企画部 所属
現在，セキュリティ関連の事業開発に従事
CISA，CISM

坂倉 基司
日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
サイバーセキュリティ技術本部 セキュリティ人財統括センタ 所属
現在，サイバーセキュリティ人財育成業務に従事

仲野 亮
日立製作所 サービス&プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
サイバーセキュリティ技術本部 セキュリティ人財統括センタ 所属
現在，サイバーセキュリティ人財育成業務に従事